

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 1 1 月 2 6 日
Date of Application:

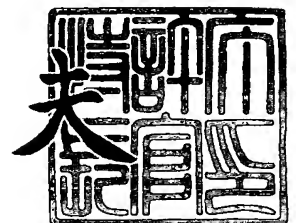
出 願 番 号 特 願 2 0 0 2 - 3 4 1 8 7 7
Application Number:
[ST. 10/C]: [J P 2 0 0 2 - 3 4 1 8 7 7]

出 願 人 株式会社日立製作所
Applicant(s):

2 0 0 3 年 1 1 月 1 4 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康





【書類名】 特許願

【整理番号】 NT02P0628

【提出日】 平成14年11月26日

【あて先】 特許庁長官 殿

【国際特許分類】 G06K 19/00

【発明者】

【住所又は居所】 神奈川県秦野市堀山下1番地 株式会社日立インフォメーションテクノロジー内

【氏名】 安藤 和則

【発明者】

【住所又は居所】 神奈川県海老名市下今泉810番地 株式会社日立製作所 インターネットプラットフォーム事業部内

【氏名】 山内 浩司

【発明者】

【住所又は居所】 神奈川県秦野市堀山下1番地 株式会社日立インフォメーションテクノロジー内

【氏名】 柴田 康久

【発明者】

【住所又は居所】 神奈川県秦野市堀山下1番地 株式会社日立インフォメーションテクノロジー内

【氏名】 大島 利喜

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社日立製作所

【代理人】

【識別番号】 100068504

【弁理士】

【氏名又は名称】 小川 勝男

【電話番号】 03-3661-0071

【選任した代理人】

【識別番号】 100086656

【弁理士】

【氏名又は名称】 田中 恭助

【電話番号】 03-3661-0071

【選任した代理人】

【識別番号】 100094352

【弁理士】

【氏名又は名称】 佐々木 孝

【電話番号】 03-3661-0071

【手数料の表示】

【予納台帳番号】 081423

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要



【書類名】 明細書

【発明の名称】 不正使用防止機能付き IC カード

【特許請求の範囲】

【請求項 1】

IC カードの所有者本人の照合に使用するバイオメトリックスデータの照合機能を備えた IC カードであって、使用可能状態となった後の IC カードの継続使用の条件を複数のパラメータにより設定可能な機能を有する IC カード。

【請求項 2】

IC カードの所有者本人の照合に使用するバイオメトリックスデータの照合機能を備えた IC カードであって、使用可能状態となった後の IC カードの継続使用の条件を、IC カードの使用後に、読み込んだバイオメトリックスデータのみを消去するまでの時間と、IC カードの使用目的もしくは使用環境との組み合わせで設定可能とした IC カード。

【請求項 3】

IC カードの所有者本人の照合に使用するバイオメトリックスデータの照合機能を備えた IC カードであって、使用可能状態となった後の IC カードの継続使用の条件を、IC カードの使用目的とセキュリティレベルの組み合わせで設定可能とした IC カード。

【請求項 4】

IC カードの所有者本人の照合に使用するバイオメトリックスデータの照合機能を備えた IC カードであって、使用可能状態となった後の IC カードの継続使用の条件として、セキュリティレベルを時間の経過とともに変化させるように設定可能とした IC カード。

【請求項 5】

所有者本人を確認できるバイオメトリックス認証モジュールを備え、予め登録しておいた所有者のバイオメトリックスデータと照合する機能と、IC カードを使用する時に所有者本人のバイオメトリックスデータを読み込み登録してあるバイオメトリックスデータと比較照合し一致した場合に IC カードを使用可能にする機能と、読み込んだバイオメトリックスデータのみを所定時間経過後に消去し

ICカードの使用時間を限定する機能と、該所定時間を任意に設定可能な機能とを有するICカード。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ICカードおよびICカードを使用するシステムに関するものである。

【0002】

【従来の技術】

情報社会において、パーソナルコンピュータなどの情報機器からインターネットを利用して電子決済や情報交換をする場が増えており、不正使用やなりすましを防止するため、パスワードや磁気カードよりセキュリティ機能の高いICカードによる所有者本人の確認が行われている。

【0003】

ICカードにおいても、紛失・盗難等の場合は所有者本人を照合するすべがなく、不正・なりすまし使用を防止するには至らない。このため、ICカード自体に所有者を特定する機能が望まれる。特許文献1及び特許文献2には、所有者本人の指紋を検出するモジュールと、予め登録しておいた指紋と照合する機能をICカードに備え、ICカードを使用する時に本人の指紋を読み込み登録してある指紋と一致した場合にICカードが使用可能となる発明が記載されている。

【0004】

特許文献3には、真のカード所持者以外の人物によるICカードの継続的な不正利用を防止することを目的として、カード所持者の認証終了後認証有効状態を示すセキュリティステータスが所定の時間だけ持続するようにし、また、上記所定の時間を経過した後、セキュリティステータスを元に戻す、あるいは該当するアプリケーションファイルを閉塞するようにした発明が記載されている。

【0005】

【特許文献1】

特開2000-36027号公報

【特許文献2】

特開 2002-150256 号公報

【特許文献3】

特開平 11-306301 号公報

【0006】

【発明が解決しようとする課題】

上述した特許文献1や特許文献2では、ICカードに所有者本人の指紋を検出するモジュールと、予め登録しておいた指紋と照合する機能をICカードに備え、ICカードを使用する時に本人の指紋を読み込み登録してある指紋と一致した場合にICカードが使用可能となる機能においても、指紋を読み取って使用可能となった状態のICカードを紛失・盗難した場合には不正使用・なりすまし使用が防止できない。

【0007】

例えば、特許文献1では、ICカードの本人の指紋を読み込み、登録してある指紋と一致した場合にICカード本体の駆動をONにする機能を有するが、使用後の有効期限に関しての配慮がなされていない。同様に、特許文献2においても、使用後の有効期限に関しての配慮がなされていない。そのため、照合後にICカードを紛失した場合、有効期限の値によっては紛失・盗難の場合には不正使用・なりすまし使用を防止できない。

【0008】

一方、特許文献3においては、ICカードにおいて所有者本人による認証終了後、認証有効状態を示すセキュリティステータスが所定の時間だけ持続するように構成されている。しかし、認証有効状態の期間、言葉を変えると、本人照合後にICカードを紛失・盗難した場合に不正使用・なりすまし使用を防止するために効果的な有効期間、は一律ではない。有効期限の値によっては、ICカードの用途・使い方が限定されてしまい、これにより、ICカードの使い勝手が損なわれたり、あるいは十分なセキュリティレベルを確保しにくくなることなどが考えられる。

【0009】

そこで、本発明は上記要望に対処し、ＩＣカードにおいて所有者本人が照合した後に紛失、あるいは盗難にあった場合でも、不正使用・なりすまし使用（以下、単に不正使用と略す場合も有）を防止でき、しかも、使い勝手が良く、かつ、十分なセキュリティレベルを確保できるＩＣカードを提供することを目的とするものである。

【0010】

【課題を解決するための手段】

本発明は、ＩＣカードの所有者本人の照合に使用するバイオメトリックスデータの照合機能を備えたＩＣカードであって、使用可能状態となった後のＩＣカードの継続使用の条件を複数のパラメータにより設定可能な機能を有する正使用防止機能付きＩＣカードに特徴がある。複数のパラメータとは、例えば、有効期限（時間）、ＩＣカード（またはその中の各アプリケーションプログラム）の使用目的、セキュリティレベル、ＩＣカード（またはその中の各アプリケーションプログラム）の使用環境等が挙げられる。これらのパラメータのは、予め、各々１つまたは複数用意されており、継続使用できる有効期限やそれをさらに継続させる条件を、有効期限と他のパラメータとの組み合わせで設定するものである。

本発明におけるＩＣカードは、所有者本人が確認できるバイオメトリックス（人間の指紋、声紋、虹彩紋、網膜紋等）認証モジュールを備え、予め登録しておいた所有者のバイオメトリックスデータと照合する機能をＩＣカードに備え、ＩＣカードを使用する時に所有者本人のバイオメトリックスデータを読み込み登録してあるバイオメトリックスデータと一致した場合にＩＣカードが使用可能となる機能を備え、読み込んだバイオメトリックスデータのみを一定時間経過後に消去し、ＩＣカードの使用時間を限定する機能を有するものである。これにより一定時間経過するとＩＣカードは再度バイオメトリックスデータを照合しなければ使用できず、本人照合後に紛失・盗難した場合でも不正使用・なりすまし使用を防止することができる。

【0011】

読み込んだバイオメトリックスデータのみを消去する時間すなわち有効期限として、予め任意の時間を設定することができる。

【0012】

例えば、ＩＣカードの種々の使用目的をパラメータとし、種々の使用目的に合わせて、予め任意の時間を設定することができる。これにより、各使用目的に応じて、ＩＣカードの使用までに本人照合が必要な時間や、本人照合後に紛失・盗難し不正使用・なりすまし使用が発生する可能性のある最短時間を考慮し、ＩＣカードの使用目的や使い勝手に合った消去までの最適な時間を設定することができる。

【0013】

さらにまた、セキュリティレベルをパラメータの１つとし、バイオメトリックスの本人照合におけるセキュリティレベルを複数のセキュリティレベルの中から選択可能にする。例えば、指紋であれば照合する特徴のレベルや、照合に使用する指の数を、ＩＣカードの使用目的に合わせて変更するように設定することができる。

【0014】

あるいは上記を組み合わせ、バイオメトリックスのセキュリティレベルと、バイオメトリックスデータのみを消去する時間設定機能を組み合わせること等で、よりＩＣカードの使用目的や使い勝手に合った本人照合及びセキュリティのレベルに設定することが可能である。

【0015】

【発明の実施の形態】

以下、本発明の実施の形態について図面を用いて説明する。

【0016】

図１は、本発明の一実施例になるバイオメトリックスデータを読み取る機能を備えたＩＣカードの概略図である。図２は、図１のＩＣカード内の各機能部位をブロック図にて説明したものである。図３は、本発明の一実施例になるＩＣカードにおいて、バイオメトリックスデータを読み取り、一定時間使用可能とする機能をフローチャートにて説明した図である。

【0017】

まず、図１において、本実施例におけるＩＣカードの概要について説明する。

本実施の形態において、ＩＣカード１は指紋認証モジュール２を表面に１個備える。指紋認証モジュール２は、所有者本人の確認を行う目的に使用するため、本実施例ではバイオメトリックスデータとして指紋を例にしているが、他のバイオメトリックスである声紋、虹彩紋、網膜紋等でも良い。また、指紋認証モジュール２は、静電気方式、光学方式のいずれでもよいが、指紋モジュール２を小さく且つ薄くしたい場合は、静電気方式であることが望ましい。

【0018】

認証に際しては、指紋認証モジュール２に所有者本人の指をのせ指紋データを読み取り、予め登録してあった所有者の指紋データと照合する。照合結果が一致した場合は、状態表示ランプ３が点灯しＩＣカード１が使用可能な状態であることを表示する。状態表示ランプ３が消灯している場合は、ＩＣカード１が使用可能ではないことを意味する。本実施例では、状態表示ランプ３はＬＥＤ等のランプであるが、使用可能かどうかを所有者に知らせることのできる機能があればよい。例えば、小型の液晶モジュールを実装して、液晶画面に使用可能状態を表示する方式、またはスピーカやブザー等を実装して使用可能となった場合に音声ガイダンスやブザー音で知らせる方式にしてもよい。

【0019】

ＩＣチップ４は、図示にないＩＣカードリーダライタ装置により、ＩＣカード１を読み取るためのモジュールである。本実施例では、ＩＣカード１はＩＣチップを使用した接触タイプであるが、無線通信機能を使用した非接触タイプでも構わない。

【0020】

図２において、本実施例におけるＩＣカード内の各機能を部位毎にブロック図にて説明する。メモリ６は、ランダムアクセスメモリ等の書き換え可能なメモリであり、所有者本人の指紋データを保存する。メモリ７は、制御部５が各種の制御を実施するうえで必要な制御プログラムや、制御データおよび設定値等の固定データが記録されているリードオンリーメモリである。制御部５は、指紋データの保存と照合および消去、各種アプリケーションプログラムを含む各種プログラムの実行、状態表示ランプおよびＩＣチップの制御、タイマ監視によるＩＣカー

ドの使用制御等を統合して制御する。電池 8 は、制御部 5、指紋モジュール 3、I C チップ 4、状態表示ランプ 3 を動作させるために必要な電力を供給するためのものである。

【0021】

次に、本実施例における I C カードの動作について説明する。始めに、I C カード 1 に搭載された指紋認証モジュール 2 にて所有者本人の指紋を読み取り、指紋データ 9 を登録しておく。指紋認証モジュール 2 にて読み取った指紋データ 9 は、制御部 5 を介してメモリ 6 に保存され、所有者のデータとして登録される。次に所有者が I C カード 1 を使用するとき、指紋認証モジュール 2 にて所有者本人の指紋を読み取り、指紋データ 10 を制御部 5 を介してメモリ 6 に保存する。

【0022】

保存された指紋データ 10 と、予め所有者のデータとして登録された指紋データ 9 を制御部 5 が比較し、データが一致した場合のみ I C カード 1 が使用可能となり、制御部 5 が I C チップに必要な信号またはデータを送信する。また、制御部 5 は I C カード 1 が使用可能状態となった時、状態表示ランプ 3 を点灯させ、所有者に使用可能状態となったことを知らせる。その後、制御部 5 は時間監視を行い、一定時間経過後に使用状態を解除し、メモリ 6 に保存していた指紋データ 10 を消去する。同時に状態表示ランプ 3 を消灯させ、所有者に使用できない状態となったことを知らせる。このことにより、使用可能状態となった I C カード 1 を紛失・盗難した場合でも、所有者本人の指紋データを再度読み取らせる必要があるため、所有者以外の不正使用・なりすまし使用を防止することができる。

【0023】

指紋認証モジュール 2 にて所有者本人の指紋を読み取り使用可能状態となつてから、使用状態を解除するまでの継続使用可能条件、ここでは時間（有効期限）は、1 分間から 5 分間くらいの短時間であることが、不正使用・なりすまし使用を防止する観点からは望ましい。解除時間の設定はメモリ 7 に記録した解除時間設定値を変更することで、I C カードの用途に合った時間に設定できる。

【0024】

なお、解除時間設定値は、I C カードの使用までに本人照合が必要な時間や、

本人照合後に紛失・盗難し不正使用・なりすまし使用が発生する可能性のある最短時間を考慮して、ＩＣカードの使用目的や使い勝手に合った消去までの時間を設定することができる。

【0025】

また、本実施例によれば、バイオメトリックスの本人照合におけるセキュリティレベルを、ＩＣカード（またはその中の各アプリケーションプログラム）の使用目的に合わせて変更するように設定する機能を有する。例えば指紋照合であれば、指紋の特徴を何ヶ所で照合するかを設定可能にすることで、所有者以外の類似の指紋に対する誤認識・不正使用を防止できる。また、指紋照合に使用する指の本数を増やしたり、指紋照合の指の順序を予め登録したりすることで、セキュリティレベルの強弱を設定することが可能となる。セキュリティレベルの内容と設定値については、予め、制御部 5 を介してメモリ 7 に保存しておく。

【0026】

図 3 のフローチャートにて、本実施例における ＩＣカードにバイオメトリックスデータを読み取り、一定時間使用可能とする機能を説明する。ＩＣカード 1 に搭載された指紋認証モジュール 2 に、所有者の指を載せる（S100）。指紋認証モジュール 2 が所有者の指紋データを読み取り、制御部 5 を介してメモリ 6 の指紋データ 10 として保存する（S101）。メモリ 6 に予め登録してある所有者の指紋データ 9 と、保存した指紋データ 10 を制御部 5 が比較照合する（S102）。指紋データ 9 と、指紋データ 10 を比較照合した結果、不一致であった場合は指紋データ 10 を消去し S100 の状態に戻す（S103）。指紋データ 9 と、指紋データ 10 を比較照合した結果、一致した場合は ＩＣカード 1 を使用可能な状態にする（S104）。制御部 5 は ＩＣカード 1 を使用可能な状態となった後、状態表示ランプ 3 を点灯させて、所有者に ＩＣカード 1 が使用可能な状態であることを知らせる（S105）。使用可能な状態となった ＩＣカード 1 は、所有者によって図示にない ＩＣカードリーダライタ装置に挿入して使用する（S106）。

【0027】

制御部 5 は S105 の状態から時間監視を行っており、設定された時間が経過

していないか監視する（S107）。設定された時間が経過した場合は、メモリ10に保存した指紋データ10を消去し、ICカード1を使用不可状態に移行させる（S108）。また、制御部5は状態表示ランプ3を消灯させて、所有者にICカード1が使用不可状態に移行したことを知らせる（S109）。ICカード1を使用可能状態とするためには、再度所有者の指紋データを指紋認証モジュール2に読み取らせる必要がある。

【0028】

以上、本実施例によれば、所有者本人が確認できるバイOMETRICS認証モジュールを備え、予め登録しておいた所有者のバイOMETRICSデータと照合する機能と、ICカードを使用する時に所有者本人のバイOMETRICSデータを読み込み登録してあるバイOMETRICSデータと一致した場合にICカードが使用可能となる機能と、読み込んだバイOMETRICSデータのみを一定時間経過後に消去し、ICカードの使用時間を限定する機能とを有しているので、本人が照合し使用を開始した後一定時間経過するとICカードは再度バイOMETRICSデータを照合しなければ使用できず、本人照合後に紛失・盗難した場合でも不正使用・なりすまし使用が防止することができる。

【0029】

また、読み込んだバイOMETRICSデータのみを消去する時間は、そのICカードの使用目的に合わせて、任意の時間を予め設定するようにしても良い。これにより、ICカードの使用までに本人照合が必要な時間や、本人照合後に紛失・盗難し不正使用・なりすまし使用が発生する可能性のある最短時間等を考慮して、ICカード使用目的や使い勝手に合った消去までの時間を設定することができる。

【0030】

また、他の実施例として、バイOMETRICSの本人照合におけるセキュリティレベルを変更可能な機能を、時間設定機能と組み合わせることにより、ICカードの使い勝手やセキュリティレベルを向上することができる。

【0031】

例えば、銀行のキャッシュカードなどは解除時間を数秒とし、その場でキャッ

シュカードを落として隣の人に拾われても、なりすまし使用を防止する。この時数秒後に再度キャッシュカードを使用する場合は、指紋照合は低いレベルもしくは照合する指は1種類とするセキュリティレベルを低めのレベルにしておき、数分後に再度キャッシュカードを使用する場合は、指紋照合は高いレベルもしくは照合する指は数種類、且つ照合する指の順番まで登録するようなセキュリティレベルを高のレベルとするような、時間の経過と共にセキュリティレベルを上げてしまう設定が可能である。これによりICカードの使い勝手とセキュリティレベルを向上することができる。

【0032】

また他の実施例として、ICカードの使用環境を配慮した設定も可能である。すなわち、ICカードあるいはその中のあるアプリケーションプログラムが不特定多数の人のいる環境下でもっぱら使用される場合と、特定の人のみがいるような環境下でもっぱら使用される場合とでは、異なる設定にするのが好ましい。例えば、事務室内のパソコン等にICカードを差し込み、ICカードが差してある間パソコンを操作可能にする環境下では、ICカードの解除期間を1時間とし、1時間毎に本人照合を行わせるようにすることが考えられる。

【0033】

【発明の効果】

以上述べたように、本発明によれば、ICカードにバイオメトリックス認識機能を設けるとともに一定時間の使用制限機能を設けたことにより、本人照合後に紛失・盗難した場合でも、不正使用・なりすまし使用を確実に防止することができる。

【0034】

また、読み込んだバイオメトリックスデータのみを消去する時間は、そのICカードの使用目的や使用環境に合わせて、任意の時間を予め設定することができる機能を有するため、ICカードの使い勝手を損なうこともない。

【0035】

また、バイオメトリックスの本人照合におけるセキュリティレベル変更機能を時間設定機能と組み合わせることにより、ICカードの使い勝手やセキュリティ

レベルをより向上させることができる。あるいはまた、ＩＣカードの使用環境を配慮した設定を行うことにより、ＩＣカードの使い勝手やセキュリティレベルを確保することができる。

【0036】

また、継続使用時間を任意に設定できることで、第三者の不正使用・なりすまし使用を防止するだけでなく、ＩＣカード発行会社としてＩＣカード所有者の不正使用を防止することにも利用できる。例えば、電車の定期券や会員証を本人以外に貸与・譲渡したりする不正使用を防止することができる。

【0037】

また、本人照合と有効期限及びセキュリティレベルを設定できるため、他の用途として、将来的にインターネットを利用した電子投票システムの投票カードに本発明を利用することもできる。

【図面の簡単な説明】

【図１】

本発明の一実施例になるバイOMETリックスデータを読み取る機能を備えたＩＣカードの概略図である。

【図２】

図１のＩＣカード内の各機能部位をブロック図にて説明したものである。

【図３】

本発明の一実施例におけるＩＣカードにバイOMETリックスデータを読み取り、一定時間使用可能とする機能を説明するフローチャートである。

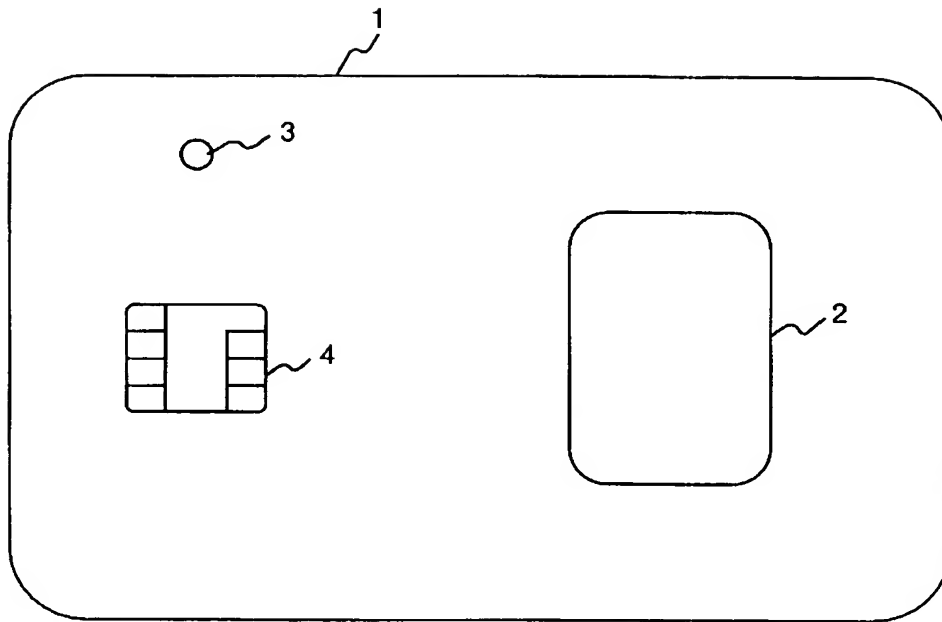
【符号の説明】

１：ＩＣカード、２：指紋認証モジュール、３：状態表示ランプ、４：ＩＣチップ、５：制御部、６：メモリ、７：メモリ、８：電池、９：指紋データ、１０：指紋データ

【書類名】 図面

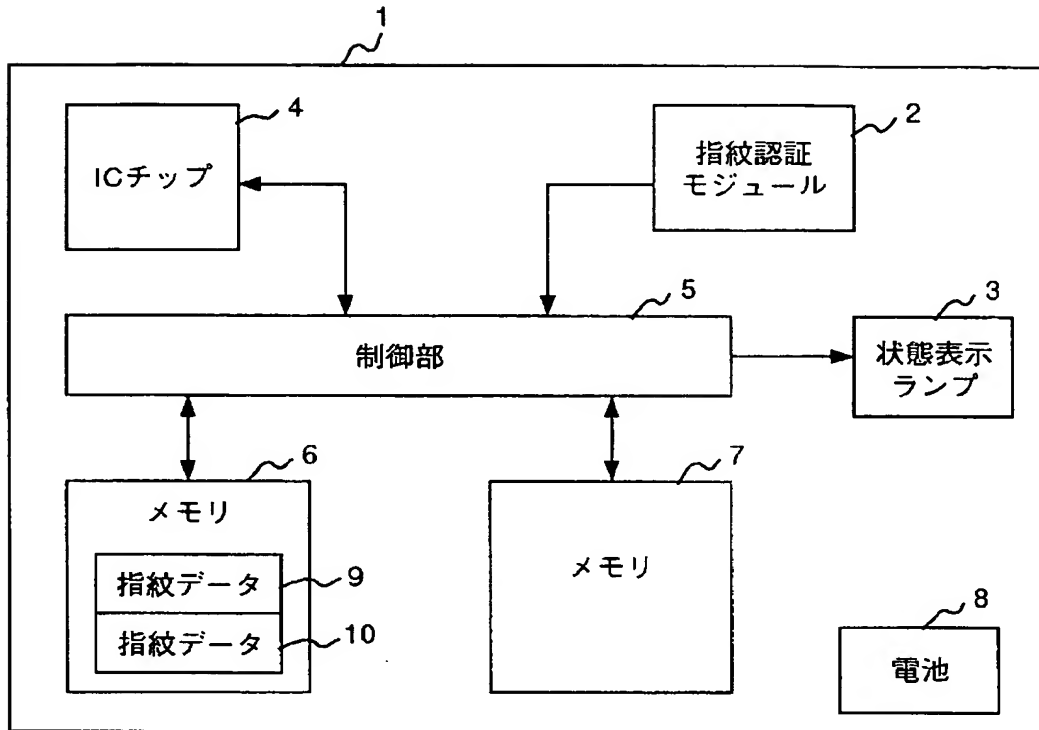
【図 1】

図 1



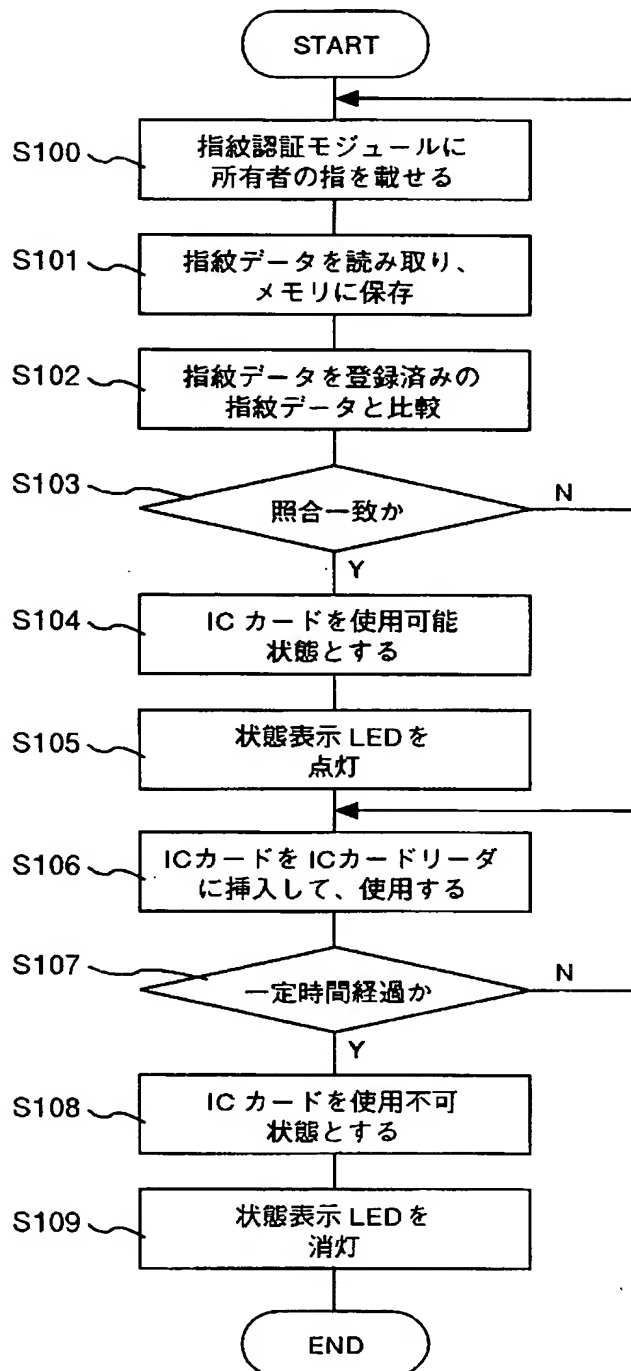
【図 2】

図 2



【図 3】

図 3



【書類名】 要約書

【要約】

【課題】

I C カードの紛失、盗難等により、所有者以外の不正使用を防止する。

【解決手段】

I C カードの所有者本人の照合に使用するバイオメトリックスデータの照合機能を備えた I C カードであって、使用可能状態となった後の I C カードの継続使用の条件を複数のパラメータにより設定可能な機能を有する。

【選択図】 図 3

特願 2 0 0 2 - 3 4 1 8 7 7

出 願 人 履 歷 情 報

識別番号

[0 0 0 0 0 5 1 0 8]

1 . 変 更 年 月 日

1 9 9 0 年 8 月 3 1 日

[変 更 理 由]

新 規 登 録

住 所

東 京 都 千 代 田 区 神 田 駿 河 台 4 丁 目 6 番 地

氏 名

株 式 会 社 日 立 製 作 所